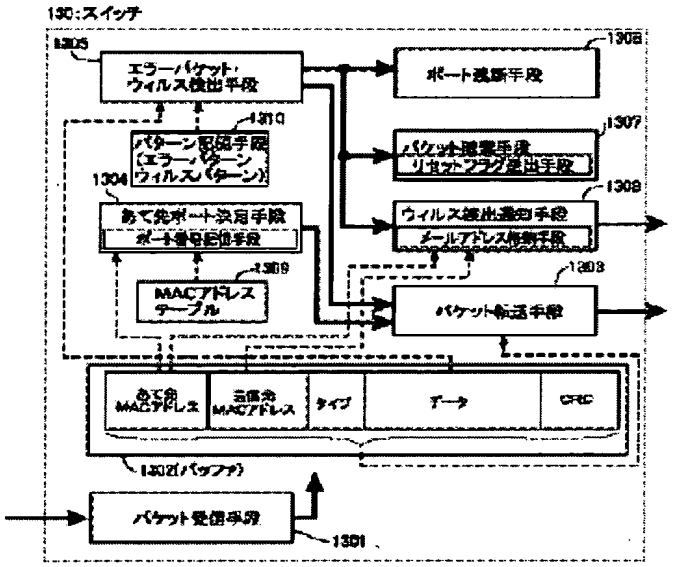
SWITCH AND LAN

Publication number: JP2003348113
Publication date: 2003-12-05
Inventor: HOSOHARA TAKESHI
Applicant: HOSOHARA TAKESHI
Classification:
- international: ***G06F21/22; G06F11/00; H04L12/46; H04L12/66;*** **G06F21/22; G06F11/00; H04L12/46; H04L12/66;** (IPC1-7): H04L12/46; G06F11/00; H04L12/66
- European:
Application number: JP20020147651 20020522
Priority number(s): JP20020147651 20020522

Abstract of **JP2003348113**

PROBLEM TO BE SOLVED: To prevent illegal packets (computer virus or the like) from being spread and expanded by detecting transmission of the illegal packets from an inside of a LAN to a WAN or delivery of them between computers in the LAN.
SOLUTION: A switch of this invention includes: (1) an illegal pattern detection means (error packet/virus detection means 1305) for detecting illegal packets from packets transmitted from computers in the LAN 100 to a WAN access apparatus and/or packets delivered among in-LAN computers; and (2) at least one of ((1)) a port shut-off means (1306) for shutting off a port, ((2)) an illegal packet abort means (1307) for aborting illegal packets, and ((3)) an illegal packet detection notice means (1308) for informing at least either of a management computer sender computer and a destination computer about detection of the illegal packets, when the illegal pattern detection means detects the illegal packets.
COPYRIGHT: (C)2004,JPO



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－348113
（P2003－348113A）
(43)公開日　平成15年12月5日(2003.12.5)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｅ	５Ｂ０７６
	２００		２００Ｓ	５Ｋ０３０
Ｇ０６Ｆ　11/00		12/66	Ｂ	５Ｋ０３３
Ｈ０４Ｌ　12/66		Ｇ０６Ｆ　9/06	６６０Ｎ	

審査請求　未請求　請求項の数５　ＯＬ　（全６頁）

(21)出願番号　特願2002－147651(P2002－147651)

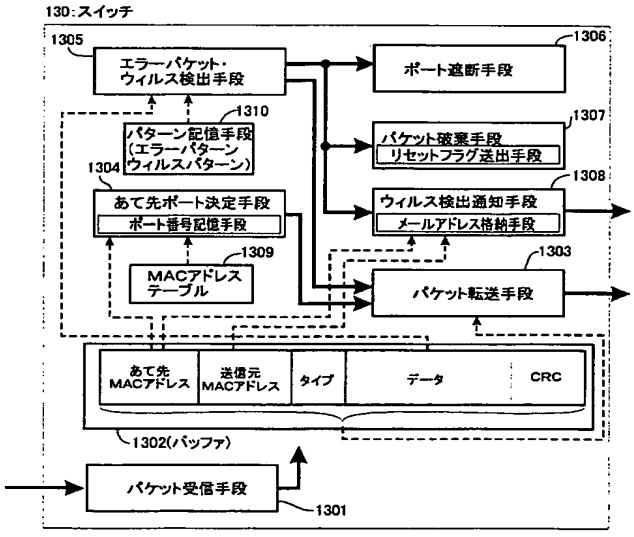
(22)出願日　平成14年５月22日(2002.5.22)

(71)出願人　502183382
細原　豪
東京都世田谷区松原６－36－17　マツモクレスト201
(72)発明者　細原　豪
東京都世田谷区松原６－36－17　マツモクレスト201
(74)代理人　100094488
弁理士　平石　利子

Ｆターム(参考)　5B076 FD08
5K030 GA15 HA08 HD06 LC18
5K033 AA08 DA06 DB18 EC04

(54)【発明の名称】　スイッチおよびＬＡＮ

(57)【要約】
【課題】　不正パケット（コンピュータウィルス等）の、ＬＡＮ内からＷＡＮへの送出や、ＬＡＮ内のコンピュータ間での受け渡しを検出することで、当該不正パケットの拡散拡大等を防止する。
【解決手段】　（１）ＬＡＮ１００内コンピュータからＷＡＮ接続装置に送出されるパケットおよび／またはＬＡＮ内コンピュータ間で受け渡しされるパケットから不正パケットを検出する不正パターン検出手段（エラーパケット・ウィルス検出手段１３０５）、（２）不正パターン検出手段が不正パケットを検出したときに、①ポートの遮断を行うポート遮断手段（１３０６）、②不正パケットを破棄する不正パケット破棄手段（１３０７）、③不正パケットの検出を管理コンピュータ送信元コンピュータ、あて先コンピュータの少なくとも１つに通知する不正パケット検出通知手段（１３０８）、の少なくとも一つの手段、を備える。



1

【特許請求の範囲】

【請求項１】　局所ネットワーク内の少なくとも１つのコンピュータを広域ネットワーク接続装置に接続し、または当該局所ネットワーク内の所定のコンピュータ間を接続するスイッチであって、

前記コンピュータから広域ネットワーク接続装置に送出されるパケット、および／または前記コンピュータ間で受け渡しされるパケットから不正パケットを検出する不正パターン検出手段、および、

前記不正パターン検出手段が前記不正パケットを検出したときに、

ポートの遮断を行うポート遮断手段、

前記不正パケットを破棄する不正パケット破棄手段、

前記不正パケットの検出を管理コンピュータ、送信元コンピュータ、あて先コンピュータの少なくとも１つに通知する不正パケット検出通知手段、の少なくとも一つの手段、を備えてなることを特徴とするスイッチ。

【請求項２】　前記不正パターン検出手段は、

複数の不正パターンを記憶する不正パターン記憶手段と、

前記不正パターン記憶手段に記憶された各不正パターンとパケットデータとを比較する比較手段と、を備えたことを特徴とする請求項１に記載のスイッチ。

【請求項３】　広域ネットワークを介して接続された不正パケットデータベースホスト装置から複数の不正パターンを取得して蓄積する不正パターンデータベースと、前記不正パターンデータベースに蓄積された不正パターンが複数セットされる請求項１または２に記載のスイッチと、を備えたことを特徴とする局所ネットワーク。

【請求項４】　前記不正パターンデータベースに蓄積された不正パターンが複数セットされる不正パケット検出サーバを介して、前記広域ネットワークに接続されてなることを特徴とする請求項３に記載の局所ネットワーク。

【請求項５】　前記スイッチにセットされた複数の不正パターンと、前記不正パケットチェックサーバにセットされた複数の不正パターンとが、少なくとも一部が異なるように選ばれてなることを特徴とする請求項３または４に記載の局所ネットワーク。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不正パケット（コンピュータウィルス等）の、局所ネットワーク（ＬＡＮ）内から広域ネットワーク（ＷＡＮ）への送出や、ＬＡＮ内のコンピュータ間での受け渡しを検出することで、当該不正パケットの拡散拡大等を防止することができるスイッチおよび局所ネットワークに関する。

【０００２】

【従来の技術】いわゆるワクチン・ソフトをインターネットに接続されたＬＡＮ内の端末コンピュータやプロクシサーバ（以下、「端末コンピュータ等」と言う）に導入することで、ＬＡＮ内の端末コンピュータ等をウィルスの感染から防ぐことができ、また、ウィルスに感染したファイルを修復することができる。

2

【０００３】ところが、上記のようなウィルス対策を、端末コンピュータ等において個別に行う場合には、各端末コンピュータ等のすべてに、ワクチン・ソフトを導入しなければならない。しかも、新種ウィルスに対しては、ワクチン・ソフトをそれぞれ頻繁にバージョンアップせねばならない。

【０００４】特に、端末コンピュータ側でウィルスの監視を行う場合には、新種ウィルスのパターンの更新やウィルスチェックの時期設定は、端末コンピュータのユーザに任されるため、ＬＡＮにおける完全なウィルス対策を実現することは容易ではない。

【０００５】このために、ＬＡＮ側のインターネットとの接続経路中にウィルスチェックサーバを配置し、ウィルスの侵入を未然に防ぐこともと行われている。この種のウィルスチェックサーバは、通過するパケットのデータをバッファに取り込み、予めレジスタ等にセットされているウィルスパターンと比較し、ウィルスチェックを行う。これにより、原理上は各端末コンピュータをウィルスの感染から防ぐことができる。

【０００６】

【発明が解決しようとする課題】しかし、実際には、ウィルスチェックサーバにトラフィックが集中した場合には、ウィルスチェックの取りこぼしが生じることがある。また、ウィルスチェックサーバでは、ＬＡＮ内でのコンピュータ間同士でのウィルスの感染を防止することができない。

【０００７】本発明の目的は、コンピュータウィルス等の不正パケットのＬＡＮからＷＡＮへの送出、またはＬＡＮ内のコンピュータ間での不正パケットの受け渡しを検出することで、当該不正パケットの拡散を防止することができるスイッチおよびＬＡＮを提供することにある。

【０００８】

【課題を解決するための手段】本発明のスイッチは、ＬＡＮ内の少なくとも１つのコンピュータをＷＡＮ接続装置に接続し、または当該ＬＡＮ内の所定のコンピュータ間を接続するものであって、前記コンピュータからＷＡＮ接続装置に送出されるパケット、および／または前記コンピュータ間で受け渡しされるパケットからコンピュータウィルスにかかる不正パケットを検出する不正パターン検出手段、および、前記不正パターン検出手段が前記不正パケットを検出したときに、ポートの遮断を行うポート遮断手段（ポートからのコンピュータの遮断、ポート自体を使用不可とする処理を含む）、前記不正パケットを破棄する不正パケット破棄手段、前記不正パケットの検出を管理コンピュータ、送信元コンピュータ、あ

て先コンピュータの少なくとも１つに通知する不正パケット検出通知手段の少なくとも一つの手段を備えてなることを特徴とする。

【０００９】本発明では、スイッチを経由して転送されるパケットに含まれる不正パターンをスイッチが検出するので、たとえばウィルスチェックサーバや端末コンピュータに導入されているウィルスチェックソフトによるウィルス検出に取りこぼしが発生するような場合であっても、極力ウィルスの検出の確度を高めることができる。なお、不正パケット検出通知手段は、管理コンピュータ、送信元コンピュータ、あるいは、あて先コンピュータに送信するときは、たとえばパケットに含まれるＩＰアドレスに基づき各コンピュータに通知を行うことができる。この場合には、通知先のコンピュータ側に対応する通信アプリケーションが備えられる。

【００１０】また、本発明のスイッチでは、前記不正パターン検出手段は、複数の不正パターンを記憶する不正パターン記憶手段と、前記不正パターン記憶手段に記憶された各不正パターンとパケットデータとを比較する比較手段とを備えることができる。

【００１１】また、本発明のＬＡＮは、ＷＡＮを介して接続された不正パケットデータベースホスト装置からコンピュータウィルス等の不正パターンを複数取得して蓄積する不正パターンデータベースと、前記不正パターンデータベースに蓄積された不正パターンが複数セットされる上記のスイッチとを備えたことを特徴とする。

【００１２】本発明のＬＡＮは、不正パターンデータベースに蓄積された不正パターンが複数セットされる不正パケット検出サーバを介して、前記ＷＡＮに接続することができる。この場合、不正パケット検出サーバと、本発明のスイッチとは、同一の不正データパターンをチェックすることもできるし、非同一の（異なる）不正データパターンをチェックすることもできる。不正パケット検出サーバと、本発明のスイッチとが、非同一または一部非同一（一部同一）の不正パターンをチェックすることでＬＡＮシステム全体の不正パターンチェック動作の最適化を図ることができる。

【００１３】

【発明の実施の形態】図１は本発明のＬＡＮが、ＷＡＮ（インターネット）に接続されたシステムの説明図である。

【００１４】図１においてインターネット２００には、ゲートウェイＧＷ１を介してＬＡＮ１００が接続され、ゲートウェイＧＷ２を介してウィルスパターンデータベースサーバ３００が接続されている。ＬＡＮ１００は、ウィルスチェックサーバ１１と、コアスイッチ１２と、複数のスイッチ（図１では符号１３１，１３２で示される２つを示す）とを備えている。

【００１５】図１ではウィルスチェックサーバ１１は、ウィルスパターンデータベースサーバ３００からウィルスパターンを一定時間間隔でダウンロードしており、通過するパケットから所定のウィルスを検出することができる。

【００１６】図１のＬＡＮ１００において、コアスイッチ１２にはスイッチ１３１，１３２が分岐接続され、それぞれのスイッチ１３１，１３２には端末コンピュータやハブが接続可能に構成されている。図１では、説明の便宜上、スイッチ１３１に接続された端末コンピュータ１４１１，１４１２およびハブ１４１３が、スイッチ１３２に接続された端末コンピュータ１４２１，１４２２およびハブ１４２３がそれぞれ示されている。

【００１７】また、スイッチ１３１，１３２には、ウィルスデータベース１５１，１５２がそれぞれ接続されている。図１では、スイッチ１３１，１３２は、ウィルスデータベース１５１，１５２に、ウィルスパターンデータベースサーバ３００から、ウィルスパターンを一定時間間隔でダウンロードしている。

【００１８】図２は、スイッチ１３１，１３２（図２では符号１３０で示す）の機能ブロック図であり、パケット受信手段１３０１と、パケットバッファ１３０２と、パケット転送手段１３０３と、あて先ポート決定手段１３０４と、エラーパケット・ウィルス検出手段（本発明の不正パターン検出手段としても機能する）１３０５と、ポート遮断手段１３０６と、パケット破棄手段（本発明の不正パケット破棄手段としても機能する）１３０７と、ウィルス検出通知手段（本発明の不正パケット検出通知手段）１３０８と、ＭＡＣアドレステーブル１３０９と、パターン記憶手段１３１０とを備えている。

【００１９】あて先ポート決定手段１３０４は、ポート番号記憶手段を備えており、ウィルス検出通知手段１３０８は、管理コンピュータのメールアドレスを格納する手段を備えることができ、パケット破棄手段１３０７は、パケットを廃棄したときにリセットフラグ（パケットを破棄した旨を示す信号）を送出するリセットフラグ送出手段を備えることができる。また、ＭＡＣアドレステーブル１３０９には、図３（Ｃ），（Ｄ）に示すように、ポート番号と、各ポートに接続された端末コンピュータ等のＭＡＣアドレスが記録される（なお、コアスイッチ１２も、図３（Ｂ）に示すようなＭＡＣアドレステーブルを有している）。

【００２０】あて先ポート決定手段１３０４は、ＭＡＣアドレステーブル１３０９を参照して、あて先ポートを決定することができる。あて先ポート決定手段１３０４は、ＭＡＣアドレステーブル１３０９にあて先のＭＡＣアドレスが書き込まれていないときは、ポートに接続されている端末コンピュータ等の全てにパケットを送信する（すなわち、フラッディングを行う）。あて先ポート決定手段１３０４は、あて先記憶手段を備えており、決定したあて先は当該記憶手段に一時記憶される。

【００２１】以下に、図２のスイッチ１３０の作用を、

図３および一部図４を参照して説明する。なお、スイッチ１３０の処理の全部をソフトウェアで行うこともできるし、処理の全部または一部をハードウェア（ＡＳＩＣ）で行うこともできる。

【００２２】図３（Ａ）は、パケットフォーマットを示している。パケット受信手段１３０１がパケットを受信すると、当該パケットはパケットバッファ１３０２に格納される。

【００２３】パケットバッファ１３０２にパケットが取り込まれたときは（図４のＳ１０１）、エラーパケット・ウィルス検出手段１３０５は、パターン記憶手段１３２０に記憶されたエラーパターンを参照して、受信したパケットのエラーパターンをチェックする（Ｓ１０２）。受信したパケットがエラーパケットである場合（Ｓ１０３の「ＹＥＳ」）には、当該パケットを破棄し（Ｓ１０４）、エラーパケットでない場合（Ｓ１０３の「ＮＯ」）には、エラーパケット・ウィルス検出手段１３０５は、パターン記憶手段１３２０に記憶されたウィルスパターンを参照して、受信したパケットのウィルスパターンのチェックを行う（Ｓ１０５）。ウィルスパターンが検出されないときは（Ｓ１０６の「ＮＯ」）、パケット転送手段１３０３は、宛先ポート決定手段１３０４の決定に従って宛先ＭＡＣアドレスに対応するポート（あて先記憶手段に記憶されているポート番号に応じたポート）にパケットを送信する（Ｓ１０７）。

【００２４】ステップＳ１０５においてウィルスパターンが検出されたときは（Ｓ１０６の「ＮＯ」）、①送信元コンピュータが接続されているポートの遮断スクリプト、②パケット破棄スクリプト、③ＬＡＮ１００内の管理コンピュータへのウィルス検出の通知（警告）スクリプトの少なくとも一つのスクリプトによる処理を選択し（Ｓ１０８）、当該選択した処理を実行する（Ｓ１０９）。なお、①のスクリプトは図２のポート遮断手段１３０６に、②のスクリプトは図２のパケット破棄手段１３０７に、③のスクリプトは図２のウィルス検出通知手段１０８に対応する。これらのスクリプトのどれを選択するかは、たとえばスイッチの管理者（あるいはシステムの管理者）等が、予め設定できる。また、上記管理者等が、適宜そのスクリプトの定義等（ポート遮断を即時に行うかの設定、警告の内容定義等）の変更ができるようにすることが好ましい。

【００２５】パケット破棄手段１３０７は、パケットを破棄するときは、リセットフラグ送出手段によりパケット送信元の端末コンピュータにリセットフラグを送出することができる。

【００２６】ＬＡＮ１００内の管理コンピュータは、③におけるウィルス検出の通知を受けることで、ＬＡＮ１００内の、どの端末コンピュータがウィルスによる感染したかを、通知に含まれるＭＡＣアドレスを参照して知ることができ、通知されたＭＡＣアドレスからＬＡＮ１００内でのウィルス感染の経路や感染状況を把握することができる。通常は、エラーパケット・ウィルス検出手段１３０５によるウィルス検出よりも前に、パケットが送信されることはない。しかし、スイッチ１３０にトラフィックが集中すること等により、エラーパケット・ウィルス検出手段１３０５によるウィルス検出がパケットのポートからの送信に間に合わず、パケット送信後にウィルスが検出されることもある。この場合には、ポート遮断を直ちに行い、またはウィルス検出通知手段１０８による通知の後にポート遮断を速やかに行うことができる。

【００２７】上記の例では、ウィルス検出通知手段１０８は、ウィルス検出を管理コンピュータに通知しているが、パケットに含まれるＩＰアドレスに基づき、送信元コンピュータ、あるいは、あて先コンピュータにウィルス検出を通知することもできる。この場合には、通常、送信元コンピュータ、あるいは、あて先コンピュータにコンピュータに対応する通信アプリケーションを導入しておく必要がある。

【００２８】図１に示したシステムでは、ゲートウェイＧＷ１にトラフィックが集中した場合には、ウィルスチェックサーバ１１におけるウィルス検出に取りこぼしが生じることがある。エラーパケット・ウィルス検出手段１３０５がウィルスチェックに際して参照するウィルスパターンと、ウィルスチェックサーバ１１がウィルスチェックに際して参照するウィルスパターンとを同一とすることで、上記の取りこぼしによるウィルス感染を回避することができる。もちろん、エラーパケット・ウィルス検出手段１３０５がウィルスチェックに際して参照するウィルスパターンと、ウィルスチェックサーバ１１がウィルスチェックに際して参照するウィルスパターンとを非同一または一部非同一とすることで、システム全体のウィルス検出の最適化を図ること（これにより転送速度が低下することを防止すること）ができる。なお、上記実施形態では、コアスイッチ１２はウィルス検出機能は備えていないが、コアスイッチ１３にウィルス検出機能を持たせることもできる。

【００２９】

【発明の効果】本発明のスイッチでは、コンピュータウィルス等の不正パケットのＬＡＮからＷＡＮへの送出、またはＬＡＮ内のコンピュータ間での不正パケットの受け渡しを検出し、不正パケットが検出されたときはポートの遮断、管理コンピュータへの通知をただちに行うので、当該不正パケットの拡散を効率よく防止することができる。

【００３０】本発明のＬＡＮシステムでは、ウィルスチェックサーバによりウィルスのチェックを行うとともに本発明のスイッチによりウィルスのチェックを行うことができるので、ウィルスチェックをより完全に行うことができる。しかも、ＬＡＮ内の端末コンピュータ間でや

7

り取りされるパケットについてウィルスチェックを行うので、ＬＡＮ内での感染拡大を防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態を示すネットワークシステムを示す図である。

【図２】本発明のスイッチの一実施形態を示す機能ブロック図である。

【図３】（Ａ）はパケットのフォーマット図、（Ｂ）～（Ｄ）はスイッチのＭＡＣアドレステーブルを示す図である。

【図４】図２のスイッチの処理を説明するためのフローチャートである。

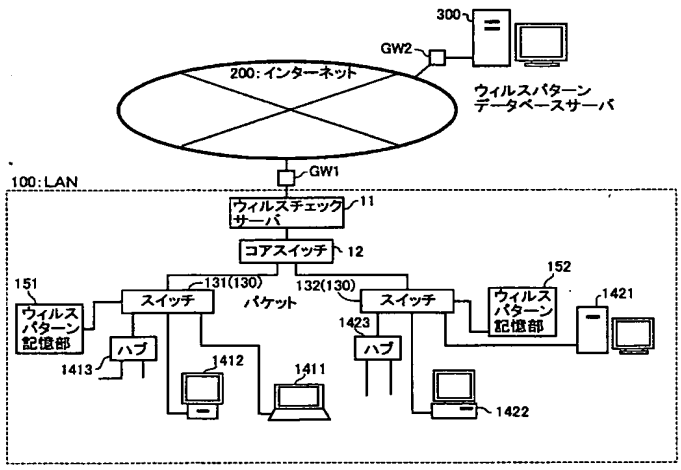
【符号の説明】

１００　ＬＡＮ
２００　インターネット
３００　ウィルスパターンデータベースサーバ
１００　ＬＡＮ
１１　ウィルスチェックサーバ

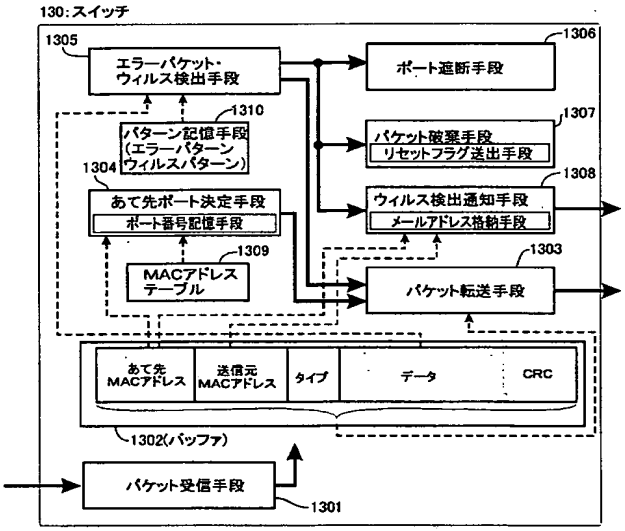
8

１２　コアスイッチ
１３１，１３２（１３０）　スイッチ
１４１１，１４１２，１４２１，１４２２　端末コンピュータ
１４１３，１４２３　ハブ
１５１，１５２　ウィルスデータベース
１３０１　パケット受信手段
１３０２　パケットバッファ
１３０３　パケット転送手段
１３０４　あて先ポート決定手段
１３０５　エラーパケット・ウィルス検出手段
１３０６　ポート遮断手段
１３０７　パケット破棄手段
１３０８　ウィルス検出通知手段
１３０９　ＭＡＣアドレステーブル
１３１０　パターン記憶手段
ＧＷ１，ＧＷ２　ゲートウェイ

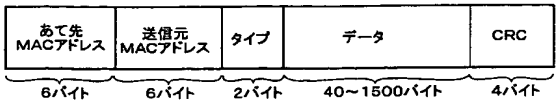
【図１】



【図２】



【図３】



(A)

(B)

コアスイッチ12のMACアドレステーブル

ポート	MACアドレス
1	A1
2	A2
3	A3

(C)

スイッチ131のMACアドレステーブル

ポート	MACアドレス
1	B1
2	B2
3	B3

(D)

スイッチ132のMACアドレステーブル

ポート	MACアドレス
1	C1
2	C2
3	C3

【図４】